7.1.3.10 Self-Diagnosis Function

The integrity of digital I&C components is continuously checked by their self-diagnostic features which consist of the following two types of detection functions. DCD_07.01-46 S01

- Detection functions performed by CPU software which performs safety functions MIC-04-07-00001
- Detection functions (include watchdog timers [WDTs]) performed by independent devices (FPGA, firmware or hardwired circuits) other than CPU software ~~software-based detection functions and hardware based detection circuits watchdog timers [WDTs].~~ DCD_07.01-46

These self-diagnostic features result in early detection of failures and allow on-line repair that improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. If any failures that disable safety functions are detected by these self-diagnostic features, alarms are generated in the MCR and safety-related signals are forced into a predetermined safe status, such as, “fail-safe” for reactor trip signals and “fail as-is” for the ESF actuation signals as shown in Figure 7.1-8. Lower priority alarms are generated in the MCR for other failures that do not disable ~~the~~any safety function~~s~~, such as a failure of one controller in a parallel redundant pair; where a redundant controller configuration is employed to maintain all system functions even in the presence of failures. The self-diagnosis is always working in the digital control system but does not affect system operation. Therefore, there is no impact to channel independence, system integrity and compliance to the single failure criterion during self-testing. MIC-04-07-00001 DCD_07.01-46 S01

There are numerous self-diagnostic functions ~~and~~,including WDT functions within the different modules of the MELTAC digital platform. Each WDT is continuously reset (avoiding timeout) based on the cyclical execution of the module's function. A WDT ~~time-out~~timeout occurs when the cyclical execution is interrupted, indicating a failure. ~~The~~Each WDT consists of a ~~hardware~~ counter, a ~~hardware~~ clock generator, and a ~~hardware~~ WDT timeout monitor, which includes a predefined timer value for WDT timeout. ~~The hardware circuits of the~~ DCD_07.01-46 S01 MIC-04-07-00001 DCD_07.01-46

Dedicated ~~WDT are independent from~~WDTs are installed in the CPU Module, the Bus Master Module, the Control Network I/F Module and the DO Module. A failure of the software (both basic and application) and the processing system hardware circuits which execute the software of the ~~MELTAC controller that performs the safety functions. A WDT timeout within one module is detected by another module in the same controller or in another controller through loss of data communication with the failed module. This other module/controller then generates~~CPU of the MELTAC controller that performs the safety functions can be detected and the outputs forced into a predetermined fail state by WDTs which are installed in the other modules. The WDT in the CPU Module can detect a failure of the CPU functions, but the signal from the WDT is processed in the CPU Module, therefore the WDT in the CPU module is not credited to detect the failure of the CPU Module. The WDTs in the Bus Master Module and the DO Module are credited to detect the failure of the CPU Module. Also, the software architecture to perform the WDT function is different and independent from the basic and application software to execute the safety functions of the CPU, therefore the WDT can detect any errors of the software which execute the safety functions of the CPU even if assuming software CCFs. The DCD_07.01-46 S01 DCD_07.01-46 S01

WDTs in the Bus Master Module and the DO Module then generate an alarm signal for the failure. The details of the self-diagnostic functions and the WDTs are described in MUAP-07005 Subsection 4.1.5. DCD_07.01-46 S01 MIC-04-07-00001

Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are specifically provided for functions with no self-diagnosis. The integrity of the self-diagnosis is confirmed by a periodic manually initiated memory integrity check, which includes the software memory which is used for self-diagnosis. For PSMS, this software memory check requires temporarily connecting each PSMS controller to the Maintenance Network. When a PSMS controller is connected to the Maintenance Network, it is considered inoperable. The functions affected by an inoperable controller are managed by plant technical specifications. PCMS controllers are permanently connected to the Maintenance Network.

In addition, when I/O is checked by manual sensor calibration and output actuation of plant components, the digital components which are self-tested are also re-checked. This provides manual confirmation for the integrity of all digital functions. The coverage of self-diagnosis and manual test is described in MUAP-07004 Sections 4.3 and 4.4. MUAP-07005 Subsection 4.1.5.1 describes self-diagnosis. The self-testing is provided for MELTAC components of PSMS, with the exception of the conventional circuits within the I/O and PIF modules, and the touch screens of the safety VDU.

As explained above, periodic surveillance tests manually confirm that all program memory instructions are correct, including the memory that controls self-diagnosis. In addition, when the periodic I/O surveillance tests manually confirm the integrity of all digital functions, they also confirms that each controller can correctly execute program memory instructions, including memory instructions that control the self-diagnostic functions. Therefore, the combination of these surveillance tests confirms that the MELTAC self-diagnosis are fully operable.

7.1.3.11 Manual Testing, Bypasses, Overrides and Resets

Manual test features are specifically provided to allow periodic testing of all functions that are not automatically tested through self-diagnosis. This includes primarily sensor calibration, manual initiation functions, memory integrity check, and final actuation of plant components. DCD_07.09-27 These manual tests also recheck the portions of the system that are self-tested, and thereby manually confirm the integrity of self-tested components and the integrity of the self diagnostic functions. All manual tests may be conducted on-line without full system actuation and without plant disturbance. The test of output modules for plant components is conducted along with the test of plant components. Since the reliability of the digital I&C equipment is significantly higher than the reliability of the plant components, the periodic test frequency is determined by the reliability of the plant components, not the reliability of the digital I&C equipment.

Safety-related systems may be placed in a bypass operation mode to allow manual testing and maintenance while the plant is on-line. For the RPS measurement channels, automatic bypass management logic prevents multiple bypassed conditions to ensure the minimum redundancy required by the technical specifications is always maintained. For other RPS functions, train level maintenance bypasses are administratively controlled.